## PATENT ABSTRACTS OF JAPAN

(11)Publication number:

2003-005641

(43) Date of publication of application: 08.01.2003

(51)Int.CI.

G09C 1/00 H04L 9/08 H04L 12/28

(21)Application number: 2001-191559

(71)Applicant: NEC CORP

(22)Date of filing:

25.06.2001

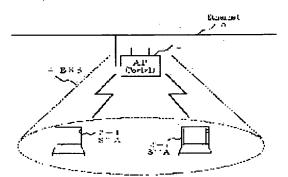
(72)Inventor: SHIMIZU MEGUMI

## (54) METHOD AND APPARATUS FOR AUTHENTICATION IN WIRELESS LAN SYSTEM

## (57) Abstract:

PROBLEM TO BE SOLVED: To provide a method and an apparatus for authentication in a wireless LAN system which can concurrently achieve delivery of an encryption key for maintaining concealment between only parties performing wireless communication and an authenticating procedure and can simplify each authenticating procedure to the same AP (a base station) performed by a S TA (a mobile terminal) completing initial authentication after releasing the authentication.

SOLUTION: The STA searches whether a MAC address of the AP intending to perform the wireless communication exists in an AP information managing table maintained by the STA. If the MAC address does not exist in the AP information managing table, a request for authenticating a public key is transmitted to the AP. If the MAC address exists in the AP information managing table, a request for re-authenticating the public key is transmitted to the AP.



## **LEGAL STATUS**

[Date of request for examination]

28.05.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

3702812

[Date of registration] 29.07.2005

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本四条件庁 (JP)

許公報(A) 那特 ধ 8

(11)特許出數公開每号 **特開2003-564**1

(P2003-5641A)

(43)公開日 平成15年1月8日(2003.1.8) (字章).十二十二 5 1 1 0 4 5K033 640Z 300E 601C 601E 1/00 8 2605 H04L

> 640 300

2605

H041

(全13月) 新水塔の数18 01 **被制裁** 人名

(71) 出版)
特置2001—191559(P2001—191559)
21)出版集号

平成13年6月25日(2001.6.25)

(22) 出版日

東京都灣区芝五丁目7番1号 日本電気株式会社 本 かんぶ A 000004237 (72) 発明者

以作件区

机大部格区芝五丁目7番1号 日本偏気株

(74)代理人 100082935

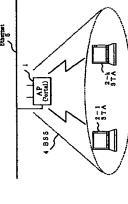
F ターム(事事) 5J104 AA07 AA18 EA08 EA19 KAD2 中華士 女本 直着 (外2名) KADS KAD6 NAD2 NA20

SRO33 AA08 CC02 DA01 DA19

(54) [発明の名称] 無様LANシスチムにおける配配方法と認証投資

た暗号用の鐵配送と認証手順の同時実現を可飽とすると 共に、初回の路配を完了したSTA(移動構来局)に関 しては、怒耐解除後の関一AP (基地局) に対する2回 目以降の認証手順の簡略化を実現可能とする、無線LA 【機題】無鋳通信を行う当事者関でのみ秘匿性を保持し Nシステムにおける認証方法と認証装置を提供する。

【解決手段】STAは、無線通信を行おうとするAPの ル内に存在するか否かを検索し、前配MACアドレスが 何配AP情報管理テーブル内に存在しない場合には、前 EA Pに対して公開機器配要求を行い、前配MACTド は、前配APに対して公開職再配配要求を行うことを特 MACTドレスがSTAの保持するAP情報管理テープ レスが約的AP情報管理デーブル内に存在する場合に



おいて、STA (移動機末局)は、無線通信を行おうと **するAP(基地局)のMACTドレスが前配STAの保 時するAP情報管理テーブル内に存在するか否かを検索** し、前記MAC7ドレスが前記AP情報管理テーブル内 ACアドレスが前記AP情報管理テーブル内に存在する 場合には、前配STAは前配APに対して公開蝦再認配 要求を行い、前記APは前記公開練再認証要求が妥当で 【職水項1】 無様LANシステムにおける認配方法に に存在しない場合には、前記STAは前記APに対して 公聚氨酚科聚水を行い、 有配A P は有配公開氨酚和聚水 が妥当である場合には前配STAの認配を行い、前配M **ある場合には前配STAの認証を行う、ことを特徴とす** る無様LANシステムにおける昭在方法。

「糖水項2」 前記AP情報管理テーブルは、前記ST Aが前記公開鐵路配要水を行って核公開鐵路配の完了與 質の有るAPのMACTドレスを最新認証完了実績類に 保持することを特徴とする情水項1に記載の無線LAN ンステムにおける認証方法。 【精求項3】 前記APは、自らの秘密録であるAP秘 STA秘密機に対応する公開機であるところのSTA公 密機と、前配AP 秘密機に対応する公開機であるところ 胚男<del>癖であるところのAPユーザ胚明書とを保</del>粹し、前 RSTAは、自らの鉛密機であるSTA秘密機と、前配 黒鍵と、前記STA公開鍵を付した自らのユーザ証明書 ことを停散とする鶴水垣1或いは鶴水垣2の何れか1項 のAP公開録と、析配AP公開機を付した自らのユーザ であるところのSTAユーザ証明書とを保持している、 こ記載の無額LANシステムにおける認証方法。

ーザ証明権を前記APに対して送信するステップと、前 【精水項4】 前配STAが前配APに対して前配公開 **製器配要求を行うステップは、公開機器配手順によって** 集成され、前記公開練認証手順は、前記STAから前配 APに対して認配要求を行うステップと、前記認配要求 を受信した前記APから前配STAに対して前記APユ -ザ証明書を送信するステップと、前記APユーザ証明 ■を受信した前配STAが、前記APユーザ証明書を検 庇した後に前配APユーザ歴明書に添付された前配AP 公開鍵を用いて前配STAューザ証明書を暗号化して暗 **身化STAユーザ証明書を作成し、前記暗号化STAユ** 記略号化STAユーザ取明物を受信した前記APが、前 記録号化STAユーザ配明春を前配AP級密鍵で復号化 して前配STAユーザ証明書を再生し、前配STAユー **ザ胚明書を検証した後に前配STAユーザ胚明書に添付** された前記STA公開鎌を用いて前記APが生成した共 画観を暗号化して暗号化共通概を作成し、 灯配暗号化共 通線を前記STAに送信して認証許可を通知するステッ プとから構成され、前配暗导化共通機を受信した前配の TAが、前配暗号化共通機を前配STA秘密鏡で復号化 **して前配共通鍵を再生し、以降のファーム暗号化通信に** 

特別2003-5641

9

族共通観を使用する、ことを特徴とする請求項3に記載 の無様しANシステムにおける認証方法

製器配要状を行う際に送受信されるMACフレーム内の フレームボゲィ街のAlgorithm Numberの値は、「0」又 【簡文項5】 射記STAが前記APに対して前記公開 は「1」でない在板の数「n」である、ことを年散とす **る簡求項4に記載の無線LANシステムにおける認証方** 

Aの認証許可時に生成し発行した共通鍵とを、最新認証 と、飲STAの前配STA公開機と、前配APが抜ST 許可順に保持する、ことを特徴とする請求項5に記載の し、 粒配公開機管理デーブルは前配A P が過去に移位所 可を通知した実権の有る机配STAのMACアドレス 【間水項6】 前配APは公開機管型アーブルを保持 無線LANシステムにおける認証方法。

**女を必信した哲配STAのMACアドレスが前記APの。** 【職米及7】 「新聞STAが前間APに対して前記公開 って構成され、前記公開機再踢駐手間は、前記STAか ら前記APに対して再路配要求を行うステップと、前記 再怒虹要求を受信した前記APが、前記公開機再路配要 し、検索した結果、前配STAのMACTドレスが前配 公開録管理テーブルに存在し、かつ、版MACアドレス に対応する公開機であるところの前配STA公開機を前 記公開機管理テーブル内に保持していることを確認した 場合には、前配APは、当該STAに対して指定する新 たな共通鏡である新共通鏡を生成し、萩新共通鏡を前配 STA公開銀で暗号化して暗号化筋共通観を生成し、該 暗号化解共通概を前配S TAに治信して認証許可を通知 するステップとから構成され、村町暗号化新共通観を受 信した前記STAが、前記暗号化新共通観を前記STA 路の最か彼中たつと哲的推共通難を再生し、以降のレフ 一ム暗号化通信に放新共通線を使用する、ことを特徴と 最再的配要水を行うステップは、公開戯再助配手順によ **する簡求項6に記載の無線LANシステムにおける認証** 保持する前記公開整管理テーブル内に存在するか検索

単再数配要求を行う際に送受信されるMACフレーム内 【簡求項8】 「和配STAが物配APに対して制配公開 と「1」と「n」でない任我の数「m」である、ことを ¥徴とする鶴水項7に記載の無線LANシステムにおけ のファームボディ筋のAlgorithm Numberの値は、「0」

【臍水項9】 無様LANシステムにおける認証装置に 3いて、無砂通信を行おうとするAP(基地局)のMA P価格管理デーブル内に存在しない場合には、前配AP に対して公国機器配要来を行い、有配MACアドレスが が配AP債報管理テーブル内に存在する場合には、 約配 Cアドレスが自身の保持するAP情報管理テープル内に 存在するか否かを複称し、ffremACアドレスがffreA APに対して公開機再認証要求を行うSTA(移動増末 €

例)と、前記STAからの対応公理書館的取求からいは 村町公理書再路的要求が収当である場合には右記STA の路配を行う前記APと、全番えることを参数とする無 禁LANンステムにおける路筒設置。

「日本のでは、 日本が同の公職を行って存べる。 日本が同の公職を行って存べ明確認在のお丁 実験の有るAPのMACアドレネを最前認在第一実験の に保持することを特徴とする ドルステムにおける認在策集。

[韓末項12] 前記STAが前記APに対して前記公 に対して認証要求を行い、前記認証要求を受信した前記 【精水項11】 析配APは、自らの約密盤であるAP 的密機と、析配AP級密機に対応する公開機であるとこ ろのAP公開瞭と、前配AP公開瞭を付した自ちのユー 析記STAは、自らの秘密機であるSTA秘密機と、前 ESTA総俗類に対応する公開難であるとにろのSTA 公開機と、前配STA公開機を付した自らのユーザ証明 る、ことを徐敬とする請求項9敗いは請求項10の何れ 開鍵路証要求を行う場合には、前記STAから前記AP APから前記STAに対して前記APユーザ証明書を設 析記APユーザ証明書を検配した後に前記APユーザ証 明書に添付された前配AP公開録を用いて前配STAユ **→ず証明書を暗号化して暗号化STAユーザ証明書を作** 成し、机能階級化STAューが配配権を利配APに対し C送信し、前記暗号化STAユーザ証明書を受信した前 記APが、前配暗号化STAユーザ証明者を前配AP秘 密録で復号化して前配STAユーザ証明書を再生し、前 記STAユーザ証明書を検証した後に前記STAユーザ 証明書に添付された前配STA公開鍵を用いて前配AP **前記暗号化共通数を前記STAに送信して認証許可を通** 知し、前配暗导化共通線を受信した前配STAが、前配 語學化共通機を耐配STA物密機で復身化して創配共通 最を再生し、以降のフレーム時号化通信に放共通録を使 用する、ことを特徴とする請求項11に記載の無線LA が配明書であるところのAPユーが配明者とを保持し、 **信し、前記APユーザ証明書を受信した前記STAが、** 4生成した共通験を暗号化して暗号化共通録を作成し、 **替であるところのSTAユーザ証別客とを保持してい** か1項に記載の無線LANシステムにおける認証装置。 Nシステムにおける認配装置。

[鶴水県13] 前記STAが前記APに対して前記な 関撃認恵要求を行う際に送受信されるMACフレーム内 のフレームボディ筋のAlgoritha Numberの値は、「0」 XII 「1」でない任務の数「n」である、ことを特数と する路水県12に配数の振襲LANジステムにおける8 8225 【鶴水項14】 が配APは公開練管理テーブルを保存し、前配公開練管理テーブルは前配APが過去に踢距野可を通わした実験の有る前配STAのMACアドレスと、「豚STAの前配STA公保鞭を、前配APが豚ST

Aの路配許可時に生成し発行した共通機とを、最新認能 年可頃に保持する、ことを特徴とする諸珠項13に配線 P無線LANシステムにおける認証装置。

管理テーブル内に存在するが検索し、検索した結果、前 存在し、から、**はMACTドレスに対応する公開職**であ 当該STAに対して指定する新たな共通機である新 RSTA秘密線で復身化して前記新共通機を再生し、以 [諸宋項15] | 前記STAが前記APに対して前記公 **積録再認証要求を行う場合には、前配STAから前配A りに対して再駆駐要求を行い、前配再認証要求を受信し** と前記APが、前記公開機再認配要水を送信した前記S 「AのMACアドレスが前配APの保持する前配公開職 RS TAのMACアドレスが前記公開機管理テーブルに るところの前配S T A 公開機を前配公開機管理テーブル 共通鍵を生成し、放新共通鍵を前配STA公開鍵で暗号 **代して暗号化新共通録を生成し、紋暗号心新共通職を前** 記STAに送信して認証許可を通知し、前記暗号化新共 B機を受信した前記STAが、前記暗号化新共通機を前 なのファーム暗号化通信に放射共通機を使用する、こと を停倒とする請求項14に記載の無機LANシステムに Aに保持していることを確認した場合には、前配AP **おける認証装置** 

【鶴本項16】 「新RSTAが創作APに対して前的公 開業再級配要求を行う癖に過受信されるMACフレーム NOフレームボディ師のMisorith Neberの信は、

ムにおける認配装置。 【発明の詳細な説明】

【発明の幹部な股別】 【免りの1】 【発明の属する技術分野】本発別は無線LANシステムにおける認配方法と認配装置に関し、特にデータを暗号化して無線通信する無線LANシステムにおいて、無線組を行う当事者間でのみ認鑑性を保持した暗号用の鍵配法と認配の同時実現を可能とする、無線LANシステムにおける認配方法と認配法を認配が表と認配法を同じまする。

[0002]

【従来の技術】無数LAN(Local Area Network:ラン)システムにおいては、滋教信するゲーケの必要指令 保存するために、滋教信するゲーケフレームの語母化が必然の条件となってきている。

「0003」無線LANシステムにおける時号化方式に ついては、これまで1EEE (Institute of Electrica land Electronics Engineers :米国、艦気/電子技術 省協会)802委員会を中心として標準化の検討が送め られてきており、その標準仕様であるIEEE802.11におい ては、無線LANにおける無線区間の毎号化及び窓匠の 方式の1つとして、Shared Key(共通戦)認配方式が探

[0004] Shared Key方式においては、<u>図1</u>に示すよ

今な振線LANの基地局としてのAP(Access Point: caP アクセスポイント)1と移動編末局としてのSTA(St Obs) ptfsにとのできる1種間の共編書を使用する、Xは1 種類の共通機を保存していない場合には、両者共通の機 特徴として4種類の共編像を保存しておき、フレーム器 APに適度を行う時には4種類の共通像を保存しているい。 ストーム語 APに適度を行う時には4種類の共通像の中の1つの共通 の名様の表別の大道像を保存している。 フレーム語 APに適度を行う時には4種類の共通像の中の1つの共通 の名様の最近が出版しては、IEEESの2、IIには了機等。 野名 作用の機の配送方法に関しては、IEEESの2、IIには定機等 5の名

【0005】Shared Key方式における路配手頃について、<u>図10及び図11</u>を参照して乾明する。

[0006] 図1のは、Shared Rey方式における際低率 職を示す図であり、図11は、Shared Rey方式の際低率 優において送受信されるフレームフォーマットのフレー ムボブイ部を示す図である。 [0007] <u>図10</u>において、AP1に対してShared K eyが式による窓面要求を行うSTA2は、AP1に対して窓配フレーム1を送着する(ステップS1)。 認能フレーム10フレームボディ部は、<u>図11</u>の(1) 認能フレーム10アレームボディ部は、<u>図11</u>の(1) 認能フレーム10アナームボディ部は、<u>図11</u>の(1) 認能ファーム11に示す形式となっており、Algoritha Naber (アルゴリズム番号) 11—1—1を「1」とし、Transaction Sequence Naber(トランデクションシーケンス番号) 11—1—2を「1」としたフレームとなっている。なお、Shared Keyが式における認能等場に、Algoritha Naber 11—11—11—11—11年に「1」であると定義されている。

[0008] ステップSIでSTA2から臨屆票本会受信したAP1は、認在フレーム2を用いてGallenge Text (チャレンジチネスト) というテンダムなピット別をSTA2に対して送信する (オテップS2)。 認在フレーム2は、図1,0 (2) 認能フレーム2に示す形式となっており、Algoritha Number 11ー2ー1は前途の通り「1」であり、Transaction Sequence Number 11ー2ー2は「2」で、Gallenge Text element (チャレンジチネストエレメント) 11ー2ー4にChallenge Text を構入したフレームとなっている。

【0009】ステップS2でAP1から認能フレーム2を受信したSTA2は、AP1から受信したChallenge fextと、WChallenge Fextに対するCRC3C(pclic Redun danor Code 32bits)算出結果に由当するICV(Integrit 7 Check Yalue:インテグリティチェック・バリュー)に 対して、共通難の1つで語号化を行う(ステップS 3)。そして、語号化したChallenge FextとICV を、使 用した共通整の整備数であるIV(Initialization Vecto

3)。よして、毎号でしたChallenge Park LICV 会、使用した共通家の整備数であるIV (Initialization Vector エムニシャルイインョン・ベクター) と共に、路筒ファーム3 母になして治療する(メアップ S4)。 既覧ファーム3 は、図110 (3) 既覧ファーム3 に大きが大くなっており、 Algorith Naber 11 ー3 ー1は巻送の通り「1」であり、Transaction Sequen

ce Number 11—3—2は「3」で、「V11—3—3、 Challenge Text element (新号化したChallenge Text) 11—3—4、ICV 11—3—5を付加したフレームと

り「1j であり、Transaction Sequence Number 11-AP 1は、受信フレーム内政情報(IV11—3—3)か 国11に示したStatus Code 11-1-9、Status Cod Code 11-4-9は、フレーム受信成功の可否などを [0010] ステップS4で認証フレーム3を受信した **らそれに対応する共通観を用いて受信ファームの暗号**化 5) と彼号結果から算出したICV の一致と、彼号結果が 5得られる平文とステップS2で送信したChallange Te ttとの一般を確認した場合には (ステップS 5 セー設を 確認した場合)、 認証フレーム4をSTA2に対して過 **着して認証完了を通知する(ステップS6)。認証フレ** - 44は、図11の(4)認能ファー44に近十形式と なっており、Algoritha Mamber 1 1―4―1 は青浴の通 e 11-2-9, Status Code 11-3-9及UStatus 4-2は「4」で、Status Code (ステータスコード) 部を復身化し、更信フレーム内ICM (ICM 11—3— 11-4-9を杆加したファームとなっている。なお、 画信相手に通知するための信頼フィールドである。

 【0012】Shared Key方式における認証と離配送の方 出した、通信を行う当事者以外の第三者(例えば軽 1つとして、通信を行う当事者以外の第三者(例えば軽 信型サージ)を介在させる年始や、他の1つとして、通 信を行う当事者のでの分配合情報の交換を行う年始があ る。前者の一例としては、時間2001—111544 場込確記載り、無数LANシステムにおける認正方社と のかか方法で十め配布し保持されば、認証サーバ と、何らかの方法で十め配布し保持されば、認証サーバ と、何らかの方法で十か配布し保持されば、認証サーバ と、何らかの方法で十か配布し保持されば、また、特 者の一例としては、特別平11-191761号公韓記 載の「相互認証方法及びその装置」が知られており、こ の公韓では、Diffie-Hollumの韓配送アルゴリズムを用 いて公課機の正当性を確認する技術が記載されている。

【知明が解決しようとする課題】第1の例として上述した整理選手・へ後利用したシステムでは、予め等勘録実動の情報を襲管選手・へに登録しておくものであり、糖配送手頭と認証手頭が分離されることにより、暗号化を半り認証手頭が接続なものとなるという欠点を有していまりの扱い接続なものとなるという欠点を有している。

[0014] また、第2の例として上述した機配送アルゴリズムを用いた認証年間においては、通信を行う当事首間でからないないでは、通信を行う当事首間でのみ過度性を保持した機配送と認証を同聴に行う

9

છ

る再度の酩飩半買実行時にも、初回の酩飩時と同一半順 多くの時間を要するものとなっており、無線伝播環境の 問題などによって通信が絶たれた際の認証解除時におけ を踏むこととなり、本米のデータ通信以外のオーバーへ ッドトラヒックを増大させてしまうという欠点を有して ことが可能となるが、その認証手順が複雑となり資算に

事者間でのみ秘匿性を保持した暗号用の鞭配法と認証手 【0015】本発明は上述した事情を改善するためにな されたものであり、本発明の目的は、無赦通信を行う当 頃の同時実現を可能とすると共に、初回の酩証を完了し AP(基地局)に対する2回目以降の認証手順の簡略化 を実現可能とする、無機しANシステムにおける認証方 たSTA(移動基末周)に関しては、競問解除後の同一 **盐と認証装置を提供することにある。** 

[0016]

【課題を解決するための手段】本発明の無線LANシス テムにおける認証方法は、無線しANシステムにおける 8位方法において、STA(移動端末局)は、無線通信 を行おうとするAP(基地局)のMACアドレスが前配 STAの保持するAP債報管理テーブル内に存在するか 否かを検索し、前配MACアドレスが前配AP情報管理 テーブル内に存在しない場合には、前記STAは前記A Pに対して公開機器紅要求を行い、前記APは前記公開 機器配要水が妥当である場合には前配STAの路配を行 い、析配MACアドレスが析配AP情報管理テーブル内 に存在する場合には、前配STAは前配APに対して公 水が妥当である場合には前配STAの認証を行う、こと 開鍵再認配要求を行い、前記APは前記公開鐵再認配要 か年数とする。

【0017】また、粒配AP情報管理テーブルは、前配 STAが前記公開機関配要求を行って蘇公開機関配の完 7実種の有るA P のMA Cアドレスを最新認配完了実績 頃に保持することを特徴とする。

ところのAP公開鍵と、前配AP公開鍵を付した自らの [0018] さらに、前記APは、自らの秘密機である AP秘密鍵と、前記AP秘密機に対応する公開機である コーザ証明書であるところのAPユーザ証明書とを保持 と、担配STA物格職に対応する公開職であるところの STA公開機と、前配STA公開機を付した自らのユー が肛明癖であるところのSTAユーザ証明癖とを保持し し、析配STAは、自らの秘密機であるSTA秘密機 ている、ことを辞散とする。

【0019】また、前記STAが前記APに対して前記 公開鐵路框要求を行うステップは、公開鐵路証手頃によ って構成され、前配公開機器配手側は、前配STAから 析記APに対して銘紅要求を行うステップと、前記認証 要求を受信した前記APから前記STAに対して前記A Pユーザ証明書を送信するステップと、前記APユーザ 胚明春を受信した前配STAが、前記APユーザ証明書

**で暗号化STAューザ配明春を作成し、前記暗号化ST** に添付された前配STA公開鍵を用いて前配APが生成 した共通録を暗号化して暗号化共通録を作成し、前配暗 引化共通験を前記STAに送信して認証許可を通知する ステップとから構成され、前配暗号化共通録を受信した 復号化して前配共通纜を再生し、以降のファーム暦号化 を検配した後に前配APコーザ配明書に終付された前配 AP公開鎌を用いて前配STAユーザ配明警を暗号化し と、前記暗号化STAユーザ証明審を受信した前記AP が、前記暗号化STAユーザ証明者を前記AP級感識で 復身化して前配STAユーザ証明審を再生し、前配ST Aユーザ証明書を検証した後に前配STAユーザ証明書 析配STAが、前配階号化共通鍵を前配STA秘密鍵で Aユーザ証明書を前配A Pに対して送信するステップ 通信に該共通鍵を使用する、ことを特徴とする。

[0020] さらに、前配STAが前配APに対して前 [0] 又は「1] でない任意の数「n」である、ことを R公開機器証要求を行う際に送受信されるMACフレー 4内のファームボディ部のAlgorithm Numberの値は、

**やし、前記公開練管理テーブルは前配APが過去に認証** 許可を通知した実績の有る前配STAのMACアドレス 【0021】また、前記APは公開練管理テーブルを保 と、抜STAの前配STA公開鎌と、前配APが挟ST Aの認証許可時に生成し発行した共通機とを、最新認証 許可順に保持する、ことを特徴とする。 幹数とする。

カフレーム暗号化通信に放新共通鍵を使用する、ことを RAPの保持する前記公別機管理テーブル内に存在する が検索し、検索した結果、前配STAのMACアドレス **最を前記公開練管理デーブル内に保持していることを確** 怒した場合には、前配APは、当校STAに対して指定 する新たな共通鍵である新共通鍵を生成し、紋新共通鍵 を前記STA公開鍵で暗号化して暗号化新共通鍵を生成 を通知するステップとから構成され、前配暗号化新共通 **建を受信した前記STAが、前記暗号化新共通録を前記** STA秘密鞭で復身だして前記第共通難を再生し、以降 [0022] さらに、 哲配STAが前配APに対して削 記公開機再認証要求を行うステップは、公開機再認証年 頃によった構成され、前配公開職再踢配手頃は、前記S 再認証要求を送信した前記STAのMACアドレスが前 が析記公開鍵管理テーブルに存在し、から、核MACア ドレスに対応する公開機であるところの前配STA公開 し、膝暗导化筋共通轍を前配STAに送信して駱缸軒可 と、前記再路配要水を受信した前配APが、前配公開側 TAから前記APに対して再認証要求を行うステップ

【0023】また、町配STAが町配APに対して村配 **讼開鍵再認証要求を行う際に送受信されるMACフレー** 「O」と「1」と「n」でない任頼の数「m」である、 A内のファームボディ部のAlgoritha Naderの値は、

ことを辞扱とする。

するか否かを検索し、前記MACアドレスが前記AP情 公開機再認配要求が妥当である場合には前配STAの認 【0024】本発明の無線LANシステムにおける認証 ドレスが自身の保持するAP情報管理テーブル内に存在 W管理テーブル内に存在しない場合には、前配APに対 して公開敷認証要求を行い、前記MACアドレスが前記 AP情報管理テーブル内に存在する場合には、前配AP と、前配STAからの前配公開機器駐要求あるいは前配 て、無検通信を行おうとするAP(基地局)のMACア に対して公開蝦再認証要求を行うSTA (移動端末周) 英層は、無線LANシステムにおける認証装置におい 匠を行う前配APと、を備えることを特徴とする。

【0025】また、前記AP情報管理テーブルは、前記 STAが前記公開機器証要求を行って該公開機器配の完 T実機の有るAPのMACアドレスを最新認証完丁実績 例に保持することを特徴とする。

AP秘密録と、前記AP秘密観に対応する公開機である [0026] さらに、前配APは、自らの秘密機である ところのAP公開機と、前配AP公開機を付した自らの と、前配STA秘密癖に対応する公開難であるところの **が配明者であるところのSTAユーザ配明者とを保持し** ユーザ胚明書であるところのAPユーザ配明書とを保持 STA公開鎌と、前配STA公開鞭を付した自ちのユー し、前配STAは、自らの総密機であるSTA級密機 ている、ことを特徴とする。

を作成し、前配籍号化STAユーザ証明を全前配APに 【0027】また、前配STAが前配APに対して前配 RAPから析配STAに対して前配APユーザ配明書を A ユーザ配明春を暗号化して暗号化S T A ユーザ配明春 対して送信し、前記暗号化STAユーザ配明春を受信し し、前配STAユーザ配明春を検証した後に前配STA ユーザ証明毎に添付された前記STA公開鍵を用いて前 配A P が生成した共通難を暗号化して暗号化共通難を作 前記共通鍵を再生し、以降のファーム暗号化通信に該共 公開機器監要求を行う場合には、前配STAから前配A Pに対して認配要求を行い、前記認配要求を受信した前 が、前記APユーザ証明書を検証した後に前記APユー **が配明書に添付された前記AP公開鍵を用いて前記ST** た前記APが、前記暗号化STAユーザ証明者を前記A 成し、前記暗号化共通機を前配STAに送信して認配幹 が、前記暗号化共通機を前記STA粉密機で復号化した 可を通知し、前配暗号化共通鍵を受信した前記STA 治信し、前記APユーザ証明書を受信した前記STA P総密機で復号化して前記STAユーザ証明書を再生 通鍵を使用する、ことを特徴とする。

【0028】さらに、前記STAが前記APに対して的 [0] 又は「1」でない任意の数「n」である、ことを 記公開鍵認証要求を行う際に送受信されるMACフレー A内のファームボディ部のAlgoritha Numberの値は、

申し、前記公開整管理テーブルは前配APが過去に認起 許可を通知した実績の有る前配STAのMACTドレス F、核STAの射配STA公開機と、前配APが核ST Aの認証許可時に生成し発行した共通機とを、最新認証 [0029] また、前記APは公路線管理テーブルを保 午可順に保持する、ことを特徴とする。

がんに存在し、かつ、彼MACアドレスに対応する公開 難であるところの前配STA公開機を前配公開機管理予 ープル内に保存していることを確認した場合には、哲配 APは、当該STAに対して指定する新たな共通録であ **5新共通鍵を生成し、放新共通機を前配STA公開糠で** を前配STAに送借して認証許可を通知し、前配暗号化、 所共通観を受信した前配STAが、前配暗号化新共通観 [0030] さらに、前配STAが前配APに対して前 RAPに対して再級船要求を行い、前配再級配要求を受 **慣した前記APが、前記公開蝦再認証要求を送信した前** RS TAのMACアドレスが前記APの保持する前記公 果、前記STAのMACアドレスが前記公開鐵管理テー **商号化して暗号化新共通概を生成し、該暗号化新共通観** 尼公開練再酩酊要求を行う場合には、前配STAから前 **製御管理テーブル内に存在するか検索し、検索した結** を打記STA 数の銀で復与化して打配解共通機を再生 し、以降のフレーム暗号化通信に終新共通鍵を使用す

[0031] ★た、単記STAが制配APに対して財配 公開鍵再認証要求を行う際に送受信されるMACフレー [0]と「1]と「n]でない缶敷の数 [m]でわる、 4内のファームボディ部のAlgoritha Numberの値は、 る、ことを特徴とする。 ことを幹板とする。

[0032]

【発貼の実施の形態】欠い、本発明の実施の形態にひず の国を参照して説明する。 [0033] <u>図1</u>は本発明の無線LANシステムにおけ [0034] <u>図1</u>に示す本実施の形態は、無様LANの ト) 1と、AP1に相属する移動機末局としての複数の の形態は、IEEE802.11で定機するところのInfrastructu ta (インフラストラクチャ) 方式であり、このような無 象LANネットワークの最小単位をBSS (Basic Serv STA (Station:ステーション) 2 (STA2-1, STA2-k)とから構成されている。図1に示す製施 基地局としてのAP(Access Point:アクセスポイン 5路配装置の一実施形態を示すプロック図である。

[0035] BSS4内におけるAP1は、各STA2 ン)ファームを、周期的にBSS4内にプロードキャス ト送信し、当校Beaconフレームを受信したBSS4内の 各STA2は、通信開始時にAP1に対して認証要求を Fv、 AP1により認証許可を受けた後、AP1への帰 84 P 1 に回数するための存储を合むBeacon(アーコ ice Set :樹木ナーガス・セット) 4か言う。

8

属処理を完了することにより、AP1との通信を行うことが可能となる。また、Infrastructumが方式におけるBSS4内の各STA2は、STA2問通信時においてもAP1を介した通信を行う。

[0036] また、<u>図1</u>におけるAP1は (cortal) となっているが、Pottalとは、IEEE902.1以外のLANプロトコルをのプロトコル変数磁能をAP1に付加したことを示しており、過速感としてのAP1とEthernet (登録膨緩) (イーナネット (登録膨緩)) 5などの有線LANとの接続を可能にした過速膨緩)) 5などの有線LANとの接続を可能にした過速膨ぶあることを示している。

[0037]なお、図1に示した実施の形態は、1828の 2.11に降助したものであるが、本実施の形態においては 無線区間の暗号化及び路配の方式として、Shared Key方 式(共通離別匹方式)とは真なり、主として秘密鍵と公 開瞭を用いた既匹方式を採用している。従って、Shared Key方式と区別するために、本実施形態における既庇方 式を公開離総配方式と便宜的に呼ぶこととする。

[0038] 次に、<u>図2を参照して、AP1とSTA2</u>の詳結構成について説明する。

ロック回である。 {0040} <u>図2</u>において、上段のプロック図がAP1 であり、下段のプロック図がSTA2である。

(10041) AD 114、図2に示す無線LANカード19ー1と L位レイナインターフェースであるところの上位レイナインターフェース17ー1を介して、てて P / I P (Transport Control Protocol/Internst Protocol/Status Foot Bを 選び、 基地局 総本本体 18 にて実現するものであり、 TA 2 は、図2に示す無線LANカード19ー2と上位 イオとのインターフェースであるところの上位レイナインターフェース 17ー2を介して、AP 1と同様な上位プロトコルの組を、/ トロパーンナルコンビュータなどの移動素本体20によって実現するものである。 [0042] 図2に示す無線LANカード19ー1と無線LANカード19ー2は、周一の構成を備える。 従って、無線LANカード19ー2は、周一の構成を備える。 従って、無線LANカード19ー2は、周のの構成を備える。 従って、無線LANカード19ー2は、同一の構成を備える。 従って、 無線LANカード19によりにあってあるのは、同一の参照数字または符号を付しておくにするものは、同一の参照数字または符号を付しておく

【0043】<u>Ø2</u>に示す無線LANカード19(19一1及び19—2)は、無線区間でのフレーム送受信を行う無線機由12と、変貨機均型を行うほび802.11 FM (Physical Layer: 物理層) プロトコル処理部13と、MAC (Medium Access Control:媒体アクセス制御 層でのアクセス制御を行う1EE592.11 MCプロトコル処理部14と、MAC層での製匠処理などの上位レイキ処理を、内臓するCPUとメモリ16によって実現する上位レイキ処理部15と、上位レイギ処理部15が使用するメモリ16とから構成されている。

1

ものとする。

【0044】女に、<u>図3を</u>参照して、STA2がAP1に対して総配を要求する際に、STA2とAP1間や治安値もれるMACファームについて観別する。

[0045] <u>図31</u>は、路匝東沖時にAPとSTA間で巻を置されるMACフレームの構成を設明する図である。
[0046] STA2のAP1に対する路距東沖時には、<u>図3</u>に示すIEEE892.11のMACフレームフォーマットに従うMACフレーム30-1は、AP1とSTA2間で交換され、MACフレーム30-1は、MAC Header (MACヘッダー)30-2と、PramaBody(フレームボイ)30-2と、PramaBody(フレームボイ)30-3とPCS(Frama Check Sequence:フレームチェックシーケンス)30-4とから構成されていったチェックシーケンス)30-4とから構成されてい

| 0 0 4 7 | そして、Infrastructure方式におけるMic Haader 3 0 - 2 は、今値フレームタイプや側架構像を示すPrense Control (プレームコントロール) 3 0 - 1 1 のフィールドと、送電光がビジーである場合に送信符機を行うための時間を推するDuration (デュレージョン) 3 0 - 1 2 のフィールドと、フレーム送信光ブドンスを示す14 Obstination Address: 送信元ブドレスを示す15 (Source Address: 送信元ブドレス を示す5. (Source Address: 送信元ブドレス を示す5. (Source Address: 送信元ブドレス 3 0 - 1 5 のフィールドと、フレーム送信段を示すSequence Control (ジーケンスコントロール) 3 0 - 1 6 のフィールドから構成される。

10048] フレーム送信等、図2に示す15E5802.11 N AGプロトコルが選番14では、上位レイギ投運街15からの送信要状プレームを、図3に示すPraneBoか 30—3に入れてかプセルビし、送信要状情報から存成した地で30(Gyzlio Redundancy Gode 32bits)算出結果を、RS 30—4としてPraneBoか 30—3の複名に付加し、ことにより、図3に示すような15E5802.11 MGプロトコルに従うMACフレーム30—1への発験を行う。続いて図2に示す15E5802.11 HIYプロトコルが運動を行う、続いて図2に示す15E5802.11 HIYプロトコルが運動を引き、は、当額MACフレーム30—1に対する変更超過を行い、無機機能12を超て当覧MACフレーム30—1を

(0049) フレーム受信時、図2に示すIEEB02, II M にプロトコル処型的14では、無線機的12を低てIEEE 002, II PHアロトコル処型的14では、無線機的12を低てIEEE 002, II PHアロトコル処型的13にて後間処理を行った 32の計算を行った 32の計算を行い、受信フレーム的のPS 30ー4の値とGC32 算出結果とが一致する場合には、M.C. Header 30ー2の内容の解析を受信フレームに対する処理を行い、Pransdody 30ー3の形分を上位レイ水処理的15。)、Pransdody 30ー3の形分を上位レイ水処理的15

[0050] 太に、<u>図4</u>及び<u>図5</u>を参照して、本実施形

第の種類な権法関係としての公認権を組みープル及びA P存集管理ケープルについて説明する。 [0051] 図4は、APが保存する公認権を選アープ の、、。

【0051】図4は、APが保持する公開験管理テープルを取明する図であり、図5は、STAが保持するAP情報管理テーブルを説明する図である。

[0052] AP1は、<u>図4に示す公開業管理テープル</u>40を、<u>図2に示す無核</u>LANカード19ー1のメモリ 16内に保砕している。公開職管理テーブル40は、A P1が過去に本契明の公開職図版において段配件可を行った実施の有る5TA2のMAC層の物型アドレスであるところのMACアドレスを保存す5SIA lac Address (STAのMACアドレス)40-1の値と、当該5TA2に入る2の金額を保存す5Public fey(パブリッタキー)40-2の値と、AP1が認配件可時に当該5TA2に対して発行した共通権を保存するNated fey(ジェア・ドキー)40-3の値とから構成されている。そして、AP1は公開機管理デーブル4の必行を、5TA2の機能認序再可能に登録する。

[0053] STA2は、図5に示すAP権報管理テーブル50を、図2に示す無線LANカード19ー2のメキリ16内に保持している。AP権報管理テーブル50は、STA2が未発明の公開機器配を要求して媒企服職器配の売了契梯の有さAP1のMACアドレスを保存するPM、MCAdress(APのMACアドレス)50ー1の補から構成されており、STA2はAP権報管型テーブル50の各行を、AP1の最新配品写真機関に発食すれる

【0054】AP1は、図4にて説明した公開練管理テーブル40への情報是影響には、監録済みのSIA MC eddess 40~1の核素を行い、既に登録済みの同一MACTドレスが存在する場合には、監録内容の情報更新となれるでアドレスが存在する場合には、監察内容の情報更新を移動する。また、本発明の公開機器配売了後のファーム時毎十0条数では、通信指令のアインが40のSIA MC eddess 40~10後報を行い、通信指令のアインが40のSIA MC eddess 40~10後報を行い、通信指令の方式の方ににより、通信指令が新いる信仰等のできた。を開業情報を開発することにより、通信指令の外表を行い、通信指令の外表を行い、通信指令の子を使びます。一次上位に位置付ることで、必要権をには、公開機管理テーブルもが現りを必要とおい通信指令の内で表も下位に位置する通信権金の表もおい通信指令の音響情報を削除することで対応する。

【0055】また、STA2はAP1と同様に 図5にて設明したAP情報管理ケーブル50~の情報是経時には、登録がみのPMC eddress 50~1の技術を行い、既に登録がみの同一MACアドレスが存在する場合には、登録内容の信報更新と共にAP情報管理ケーブル50の先頭の行へ当算情報を移動する。また、本窓明の公の方式のケーム暗号に通信の実施時に、STA2はAP情報管理テーブル50のPMC eddress 50 424AP情報管理テーブル50のPMC eddress 50 424AP情報管理テーブル50のPMC eddress 50

──1の検索を行い、通信和年のAP1の管理情報をAP 情報管理チーブル50の先頭の行へ移動するにとにより、通信報金が新しい通信相手の管理情報ほど管理デーブル上位に位置けけることで、AP情報管理デーブル50が現界登録に対し、新成情報登録が不可能となった整合には、AP情報管理デーブル50が収入可能となった画作を金の表も古い通信相手の管理情報を創除することで対応する。

[0056]女に、<u>図6、図7、図8、図8を</u>毎円 た、本実施形態の動作について観明する。 【0057】本集施形態においては、図1に示した無線 LANシステムの、基地局であるAP1と移動地系局であるSTA2は、共に、自らの秘密機とそれに対応する 公開機、及び貸公開機を添付したユーザ原野舎を帰り ているものとする。そして、当様ユーザ原野舎との保育者 機関に代表される第二者によって、公開機とその保育者 (すなわち、AP1放いはSTA2)との関係、及び保 有者自身の正当性を庇明可能である、という条件を削額 とするものとする。以下は、ユーザ原野舎は増加 とするものとする。以下は、ユーザ原野舎は野が

ューザ配明春を意味するものとする。 【のの58】<u>図1</u>におけるSTA2がAP1を介しての。 無鉄道管を行おうとする場合には、STA2は先ずAP 1に対して、本税明の公開機器配展水を送信することか ら開始する。

[0059] STA2は公開機能応開始時に、総証要求 先のAP1のMACアドレスを用いて<u>図ら</u>に示したAP 情報管理テーブル50内のNP MC Address 50一1の検 素を行い、AP情報管理テーブル50内に総証要求先A P1のMACアドレスが存在しない場合には、初回の路 配要求として<u>図ら</u>に示す公開機能配手現を行い、路取要 求先AP1のMACアドレスが存在する場合には、過去 に当該AP1との公別機能配配の完了実得が有る場合であ るため、再認証として、<u>図3</u>に示す公開機再認証手環を 179。 [0060] 先ず、初回の認証要求としての公開機認証 手順について、<u>図らみい図2</u>を奪用して説明する。 [0061] <u>図ら</u>は、公開機認証手順を示す図であり、 図<u>2</u>は、公開機認証手順において送受信されるMACフ

/ | オのファーオだが # (図3のFrameBody 30 —

9

[0063] ステップS61でSTA2から公開鍵認証 要求を受信したAP1は、認証フレーム62を用いてA P1の保持するユーザ証明書をSTA2に対して送信す (2) 認用ファーム62に水上形式となったおり、Algo る (ステップ562)。 認証フレーム62は、<u>図1</u>の

で、APのユーザ配明者70―2―3にAP1の保持する ユーザ証明書(ユーザ証明書に付加するAP1の公開機 ritha Number 70-2-1は前浴の通り「n」であり、 fransaction Sequence Number 70-2-21 12, かも付したもの) を御入したファームとなっている。

【0064】ステップS62でAP1から認能フレーム 62を受信したSTA2は、AP1から受信したAP1 のユーザ証明**律**の内容を検証して、AP1のユーザ証明 春の検証結果に問題の無いことを確認すると、AP1の ューザ証明書に添付された公開録を用いて、STA2の (3) 昭間フレーム63に示す形式となっており、Algo STA2のユーザ位明春に付随するSTA2の公開機と 共に、怒腔フレーム63を用いてAP1に対して送信す で、APO公開館で暗りたしたSIA のユーザ配明書10ー 保存するユーが配明者の暗号化を行う (ステップS6 3)。そして、暗學化したSTA2のユーザ類明書を、 る (ステップS64)。 認備フレーム63は、殴1の ritha Maber 7 0 — 3 — 1 は耐浴の通り「n」であり、 Transaction Sequence Number 70-3-2(1 [3]

3-3か年拾したソフー々となっている。

したAP1は、APの公別職で暗号化したSTAのユーザ缸 された公開鍵を用いて生成した共通鍵を暗号化する(ス アップS65)。そして暗号化した共通概を、認証ファ (4) 路局レフー464に形上形式かなしたおり、Vlgo 【0065】ステップS64で認証フレーム63を受信 明書10—3—3をAP1の総密機で復号化して、ST 今度は共通鍵を生成し、STA2のユーザ証明書に添付 ーム64を用いてSTA2に送信し、認配許可を通知す で、STA の公開機で暗号化した共通機70-4-3を付 加したフレームとなっている。なお、図2に示したStat us Code 70-1-9, Status Code 70-2-9, St atus Code 70-3-9 & UStatus Code 70-4-9 A2のユーザ証明春の内容を検証し、STA2のユーザ **配明書の検証結果に問題の無いことを確認すると、次に** ritha Marber 7 0 — 4 — 1 は哲説の誦り「n」であり、 る (ステップS66)。 昭和フレーム64は、図1の Transaction Sequence Number 70-4-212 [4] 4) } (f

[0066] その後、ステップS66でAP1から認証 フレーム64を受信したSTA2は、STA の公開鍵で暗

は、フレーム受信成功の可否などを通信相手に通知する

れむの価数レメーケドかもの。

巻を使用することとなる(ステップS67)。 以上の動 引化した共通額70-4-3をSTA2の総密機で復身 比して、AP1が生成した共通鍵を復元し、この後実際 に行われる無線通信におけるフレーム暗号化に、放共通 作により、公開難認証手頭が終了となり、以後、STA 2とAP1間でフレーム暗号化通信が行われることとな [0067] 次に、再路配が行われる際の公開離再認能 年間について、図8及び図9を参照して説明する。

り、<u>図9</u>は、公開難再認証手頃において送受信されるM ACソフームのソフーム於がィ哲(図3のFraneBody3 [0068] 図8は、公開機再路配手順を示す図であ 0-3) を示す図である。

**再路信要求としてAP1に対した怒信レレー481を泌** ムボゲィ街は、図9の(1)昭和フレーム81に示す形 **-2を「1」としたフレームとなっている。なお、公昭** 離再級配手頃における級配時には、Algorithm Number 9 0-1-1~80-2-17年に「町」(町は「0」と [0069] <u>図8</u>において、認証要求先のAP1に対し 言する (ステップS81)。 路位フレーム81のフレー 男) 90-1-1を「m」とし、Transaction Sequence 「m」とすることにより、図<u>6</u>に示した公開機器配手順 **に過去に公開機路配完丁実機のあるSTA2は、公開**線 Number (トランチケツョンツーケンス物中)90-1 式となっており、Algorithm Namber (アルゴリズム物 5. Algorithm Number 9 0-1-1~9 0-2-1を 「1」と「n」でない任意の数)であるものと定義す と区別することが可能となる。

雅殿した場合には、AP1は当該STA2に対して指定 2―1は對法の通り「m」であり、Transaction Sequen 早先した整共通難90~2~3を存在したアレームとな [0010] ステップS 8 1でSTA 2から公開競再器 に示した公開鐵管理デーブル40において、公開鐵再認 iddress 40-1に存在するが検索を行う(ステップS 82)。そして、検索が成功し、かつ、それに対応する 公開鍵をPublic Key4 0 — 2の橋に保持していることを する共通鍵を新たに生成し、この新共通鍵を公開鍵管理 アーブル40のPublic Ker40一2から取得した公開銀 **が883)。 そして、暗号化した粧共通観名、認能ファ** 4) . 酩텀レアー482は、図30 (2) 酩텀レアー4 8.2 に示す形式となっており、Algoritha Naber 9.0ー ce Number 90—2—2は「2」で、STA の公開館で掲 っている。なお、図9に示したStatus Code 90—1— )及t/Status Code 90-2-9は、フレーム受信成功 胚要求を受信したAP1は、AP1が保持している<u>図4</u> 低要求を送信したSTA2のMACT ドレスがSTA Mac (当該STA2の公開機)を用いて暗号化する (ステッ の可否などを通信相手に通知するための情報フィールド ーム82を用いてSTA2に送信する (ステップS8

ム暗号化に、放新共通雙を使用することとなる(ステッ [0011] その後、ステップS84でAP1から認配 フレーム82を受信したSTA2は、STA の公開機で暗 **号化した新共通数90−2−3をSTA2の保存する**級 密轍で復号化して、AP1が新たに生成した新共通鍵を プ585)。以上の動作により、公開蝦再路配手順が終 Tとなり、以後、STA2とAP1間でフレーム暗号化 復元し、この後実際に行われる無線通信におけるファー 画信が行われることとなる。

[0072]以上、本地配の第1の無循形観示しいた時 冊に説明した。第1の実施形態においては、AP1とS FA2が共に自らの秘密機とそれに対応する公開機、及 胚別番は路転機関に代表される第三者によって公開銀と その保有者との関係及び保有者自身の正当性を証明可能 公開機略証要求を行い、AP1から略証許可を得るまで 別に基づき、AP1とSTA2が認証完了実績のある相 り、2回目以降の認配要水時において四里に示す公開機 び公開鍵を添付したユーザ配明権を保持し、当該ユーザ であるという条件のもとで、STA2がAP1に対して こは、図6に示す公開録の交換年順が発生するが、本発 再器証手順を用いることにより、初回の器証手順で行っ とで、認配処理手順の簡略化が可能となる、という効果 たAP1とSTA2関での公開線交換手順を省略するこ 年の公開整情報を認配解除後も保持し続けることによ を有している。

おいてユーザ証明書を用いることにより、AP1はST A2の公開鏡とその保有者であるSTA2の正当性とを 無路した上での数配許可後にSTA2の公開機情報を保 に対して送信する共通観を正当なSTA2のみが保持す る秘密難に対応した公開難によって暗号化するため、成 9 すましによる再認転要求元STAはこれを復身化し共 面離を取得することができず、従って本発明によって不 【0073】また、図6に示す初回の公開機器配手頃に 図8に示す公開機再認証手順を行うAP1は、STA2 Pすることから、当該STA2のMACアドレスを使用 した成りすましによる再認証要求が発生した場合には、 EなSTAによる成りすましを防ぐことが可能となる、 という効果を有している。

【0074】代に、本発明の第2の実施形態について呪

【0075】第2の実施形態は、複数のAP (基地局)

ク内における共有情報とする構成とした無赦LANシス る構成は、例えば、複数のAPを被指する上位APを配 数し、上位APが公開鐵管選情報を一括して保粹してお し、且つ各BSS同士が有機又は無線で接続される複合 ネットワーク上において、各APに帰属中のSTA (移 **影婚末局)に関する公開報管理情報(具体的には、<u>図4</u>** に示した公開鐵管理アーブル40)を、複合ネットワー アムである。複合ネットワーク内における共有情報とす による複数のBSS (基本サービス・セット) が存在

き、各APは必要時に上位APに対する登録あるいは間 **い合わせを行い、その回答を上位APから得る構成であ** 5。このような構成とすることにより、任意APに帰属 FのSTAが、BSSの体制により他のAP〜初回の公 開鍵認証を行う際にも、本発明による公開機再認証手順 と実施することにより認証処理手順の簡略化が可能とな 5、という効果を有するものとなる。

[0076] 太に、本発明の第3の実施形態について説

【0077】 類3の実施形態は、IEE802.11で定義する ところのIndependent (インディペンデント: 強立) ガ 集成とすることにより、2回目以降の公開機再路配包組 手頃の簡略化が可能となる、という効果を有するものと 式の無線L ANシステムに第1の実施形態の本発明を適 て、IBSS内におけるSTA間での公理機関間等にお こと、本路的の第1の実権形態に魅力を、公開戦略配取 **水を受信したSTAが認証要求元STAの公開録管理情** 0) を保持し続ける構成としたものである。このような (Independent BSS :インディペンデントBSS) 内に 引する構成である。Independent 方式では、IBSS 数数のSTAだけが存在し、APは存在しない。そし 線(具体的には、図4に示した公開整管理アーブル4

[0078] なお、本発明の第1、第2及び第3の実施 形骸において、銘配許可を行うBSS内APやIBSS 内STAが保持する認証要求元STAに関する公開機會 単価機と共に、ユード間別権に拠づく在秘越原信権を選 せる構成とすることにより、有効期限切れユーザ配明権 入することによって、公院教育理情報の保存期限を特た の継続使用を防ぐことが可能となる。

認証手順の同時実現を可能とすることができるので、初 80日解除後の同一AP(基地局)に対する2回目以降の (発明の効果)以上説明したように、本発明の無線LA Nシステムにおける認配方法と認証装置は、無鉄通信を 行う当事者間でのみ銘度性を保存した暗号用の観覧法と 回の酩酊を充丁したSTA(移動端末局)に関しては、 認証手順の簡略化を実現可能とする、という効果を有し

Cいる。 【図面の簡単な説明】

[図1]本発明の無機LANシステムにおける認配装置 **ケー実施形態やポナプロック図かめる。** 

[図3] 昭証要水時にAPとSTA間で送受信されるM [図2] APとSTAの一郎を示す事権プロック図であ

図4 A Pが保持する公開機管理テーブルを散明する ACフレームの構成を説明する図である。 M + 35.

|<u>図5</u>| STAが保持するAP債保管理テーブルを説明 - 各国である。

\*) } ;

**衛課2003—5641** 

(12)

体第2003—5641

Ξ

)

Frame Body 9-2312

SA ESS D Sequence

ž

Derution

IEEE802.11 NACプロトコル処理部 IEEE802.11 PAYプロトコル処理部

上位レイヤ処理部

Ethernet (イーサネット)

BSS

[<u>図7]</u> 公開戦器駐手順において送受信されるMACフ

[<u>図9</u>] 公開舞再認証手順において送受信されるMAC

レワームのレフーム共どィ密的ドナ図かもる。 【図8】公開舞再閣配手順を示す図である。 レームのフレームボディ部を示す図である。 【図6】公開機略配手順を示す図である。

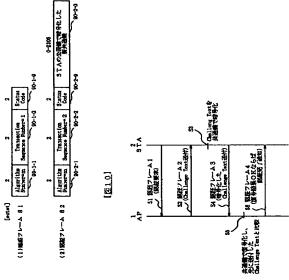
【<u>図10</u>】Shared Key方式における認証手順を示す図で

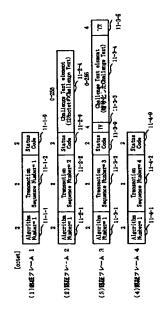
[符号の説明] 1 AP

てある.

(S)

(13)





[811]